

REMARKS/ARGUMENTS

The present Amendment is in response to the Final Office Action having a mailing date of May 26, 2005. Claims 1-22 are pending in the present Application. Applicant has amended claims 21-22. Consequently, claims 1-22 remain pending in the present application.

Applicant has amended claims 21-22 to correct a minor spelling error. Consequently, Applicant respectfully submits that no new matter is added and no new search is required.

This application is under Final Rejection. Applicant has presented arguments hereinbelow that Applicant believes should render the claims allowable. In the event, however, that the Examiner is not persuaded by Applicant's arguments, Applicant respectfully requests that the Examiner enter the Amendment to clarify issues upon appeal.

In the above-identified Final Office Action, the Examiner rejected claims 1-17 under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,792,113 (Ansell) in view of U.S. Patent Publication No. 2002/0071559 (Christensen). In so doing, the Examiner indicated that Ansell teaches that a security key pair can be associated with either machine binding (bound) or user-binding (not bound). The Examiner indicated that Ansell does not expressly disclose creating key pair material for use with an embedded security chip of a computer system. Consequently, the Examiner relied upon Christensen, paragraphs 245 and 252 for this teaching. Further, in response to Applicant's arguments, the Examiner indicated that "the collection of security key passport data structures combining with user option indicator is equivalent to the key material including tag data to meet the claim language."

Applicant respectfully disagrees with the Examiner's rejection. Claim 1 recites a method for control of key pair usage in a computer system. The method recited in claim 1 includes creating key pair material for utilization with an embedded security chip of the computer system.

The key pair material is specifically recited as including tag data. Claim 1 further recites determining whether the key pair material is bound to the embedded security chip based on the tag data. Claim 7 recites an analogous computer system including a main processor and a security processor. The security processor stores tag data with key pair material and determines binding of the key pair material to the security processor based on the tag data. Similarly, claim 16 recites a method for controlling usage of key pairs in a hierarchical structure of key pairs in an embedded security chip. Claim 16 recites storing tag data with key pair data for each level of the hierarchical structure and determining whether the key pair data is bound to the embedded security chip based on the tag data.

Thus, claims 1, 7, and 16 utilize tag data of the key pair material in order to determine the binding status of the key pair. Consequently, a user can either be bound to a particular system or may be verified securely on any system. Specification, page 7, lines 9-13.

Ansell in view of Christensen fail to teach or suggest the methods and system recited in claims 1, 7, and 16. In particular, Ansell in view of Christensen fails to teach or suggest utilizing key pair material for use with an embedded security chip, or security processor, in conjunction with determining binding of the key pair material to the embedded security chip/security processor based on the tag data.

Ansell describes a system that does allow a binding to a machine or to a user. Ansell, col. 2, lines 35-54. However, Ansell fails to teach or suggest a method or system in which key pair material includes tag data that is used in determining binding to an embedded security chip/security processor. Instead, Ansell utilizes passports. For machine binding, Ansell describes creating a passport that contains the private key for the machine and a public key for the machine. Ansell, col. 2, lines 35-38. The private key is based on a hardware identifier for the machine. Ansell, col. 2,

lines 38-40. The public key is the reciprocal of the private key. Ansell, col. 2, lines 35-38. Ansell also allows the creation of a passport for user binding. Such a passport also includes a private key and a public key that is the reciprocal of the private key. Ansell, col. 2, lines 54-64. However, the private key is based upon a password provided by the user. Ansell, col. 2, lines 56-60. Ansell further discloses changing the passport to machine binding for a passport for user binding. However, in order to do so, Ansell describes creating a *new* user passport using the keys of the machine-bound passport in conjunction with the user's password. Ansell, col. 3, lines 25-35.

Thus, it is the hardware identifier of Ansell that indicates that the keys are machine-bound. This hardware identifier is specific to a hardware device, for example a hash of the MAC address for the computer. Ansell, col. 6, lines 5-18. Similarly, it is the user password that indicates that the key is user-bound. Ansell, therefore, does not use tag data to determine whether the keys are user bound or machine bound. Instead, Ansell utilizes quantities that are effectively passwords for the machine (the hardware identifier that is unique to a particular machine) and for the user (user password). Different passports have different passwords and, therefore, different keys depending in part on whether the keys are bound to a particular machine or user bound. For example, the data indicating that a key is machine bound varies from machine to machine because the hardware identifier varies between machines. Consequently, in the system of Ansell utilizes passwords to determine whether particular keys for a particular passport are bound to a user or bound to a particular machine. Applicant respectfully submits that one of ordinary skill in the art would recognize that using different passwords for different types of binding and different passwords for machine binding to different types of machines are distinct from the recited tag data. Thus, Ansell fails to teach or suggest the recited tag data that is used to determine the binding of the key pair.

Christensen fails to remedy the defects Ansell. Christenson describes a system for decrypting content, such as copyrighted content. Christensen, Abstract and col. 1, lines 1-4. In order to do so, Christensen describes using keys. Christensen, paragraph 245. However, Applicant has found no mention in Christensen of user binding and machine binding, much less of using tags to determine whether the keys are user bound or machine bound. Both Ansell and Christensen fail to teach or suggest the use of tag data to determine whether keys are bound to an embedded security processor/security chip. Consequently, any combination of Ansell and Christensen fail to teach or suggest such a feature. Ansell in view of Christensen, therefore, fail to teach or suggest the methods and system recited in claims 1, 7, and 16.

Further, Ansell in view of Christensen fails to teach or suggest the use of an embedded security chip or processor. The Examiner has acknowledged that Ansell fails to disclose creating key pair material for utilization with an embedded security chip of the computer system. Consequently, the Examiner has relied upon paragraphs 245 and 252 of Christensen to teach the use of such an embedded security chip. However, the cited portions of Christensen merely describe providing a decryption key to a part of the processor or to an "inaccessible" part of the processor. Christensen, paragraph 245. Christensen further describes the processor as being a silicon chip or other device such as a Smart Card that can be incorporated into the other pieces of hardware. Christensen also indicates that the inaccessible portion of the processor is such that neither the user nor the computer system can see the inaccessible portion of the processor. In contrast, the specification specifically defines the embedded security processor/security chip as a "cryptographic microprocessor" that is embedded in the system board of the computer system and through which security operations are routed. Specification, page 1, lines 14-16, page 1 and line 18-page 2, line 4. Consequently, such an embedded security processor/security chip is not merely a portion of a

processor that is made “inaccessible” to a user. Such an embedded security processor/security chip is distinct from a device such as a Smart Card. Further, there is no prohibition on the embedded security chip being accessed by the computer system. Consequently, the recited embedded security processor/security chip is distinct from the inaccessible portion of the processor described by Christensen. Moreover, with respect to claim 7, Applicant notes that separate main and security processor are recited. This is also distinct from the inaccessible portion of the processor or other hardware device described by Christensen. As a result, Ansell in view of Christensen neither teach nor suggest the use of the recited embedded security processor/security chip. Ansell in view of Christensen do not, therefore, teach or suggest the methods and system recited in claims 1, 7, and 16. Consequently, Applicant respectfully submits that claims 1, 7, and 16 are allowable over the cited references.

Moreover, claim 16 recites storing tag data along with key material in conjunction with using the tag data to determine whether the key material is bound to the system. This feature is neither taught nor suggested by Ansell in view of Christensen. The cited portion of Ansell describes the ability of the system of Ansell to change a key pair from a machine-bound (bound) pair to a user-bound (not bound) pair. Ansell, col. 2, lines 28-66. To do so, the keys are stored in passports. However, the history of the keys, including the whether the key/passport has been converted from bound to unbound is stored not in the passport, but in a table in a certificate database. Ansell, col. 10, line 6-64. Applicant respectfully submits, therefore, that data relating to the nature (bound/unbound) of the key resides in the certificate database. Consequently, the cited portion of Ansell indicates that Ansell stores information regarding the binding status of the key, not with the key in the passport, but in the separate certificate database 127. Thus, Ansell

fails to teach or suggest storing tag information from which the binding state of the key material can be determined along with the key material.

Christensen fails to remedy this defect. The cited portions of Christensen do describe encryption and decryption, including storing a key material in a processor. However, Applicant has found no mention in the cited portions of Christensen of storing tags with the key material, or that such tags can be used to determine whether the key material is bound. Consequently, any combination of Ansell and Christensen would also fail to include such a feature. Stated differently, if the system of Christensen were added to the teachings of Ansell, the system of Ansell might use the inaccessible portion of the processor to perform certain aspects of encryption/decryption, including storage of key material. However, the system would still track the status of the passports and, therefore, the key material using the certificates stored in the certificate database. Consequently, Ansell in view of Christensen fail to teach or suggest storing tag data that determines whether the key material is bound along with key material. Ansell in view of Christensen thus fail to teach or suggest the methods and system recited in claims 1, 7, and 16. Accordingly, for the above-identified reasons, Applicant respectfully submits that claims 1, 7, and 16 are allowable over the cited references.

Claims 2-6 and 20 depend upon independent claim 1. Claims 8-15 and 21 depend upon independent claim 7. Consequently, the arguments herein with respect to claims 1 and 7 apply with full force to claims 2-6, 8-15 and 20-21. Claims 17-19 and 22 depend upon claim 16. Consequently, the arguments herein with respect to claim 16 apply with full force to claims 17-19 and 22. Accordingly, Applicant respectfully submits that claims 2-6, 8-15, and 17-22 are allowable over the cited references.

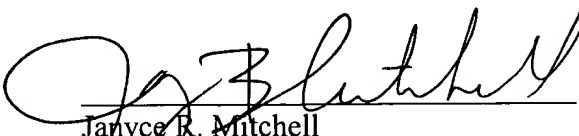
Furthermore, Applicant respectfully submits that claims 20-22 are separately allowable over the cited references. Claims 20-22 recite that the key pair materials are created or the hierarchical structure is organized such that key pair material for a portion of "each of at least two of the different levels are not bound." Applicant has found no mention in Ansell or Christensen of such a hierarchy. Consequently, any combination of Ansell and Christensen would fail to teach or suggest organizing the hierarchy or creating the key pair material such that key pair material for a portion of each of at least two of the different levels are not bound. Ansell in view of Christensen thus fail to teach or suggest the method and systems of claims 20-22. Accordingly, Applicant respectfully submits that claims 20-22 are allowable over the cited references.

Applicant's attorney believes that this application is in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicant's attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

August 4, 2005
Date


Janyce R. Mitchell
Attorney for Applicant(s)
Reg. No. 40,095
(650) 493-4540